A systems approach to cyber-risk management

Sepúlveda Estay, Daniel Alberto; Khan, Omera

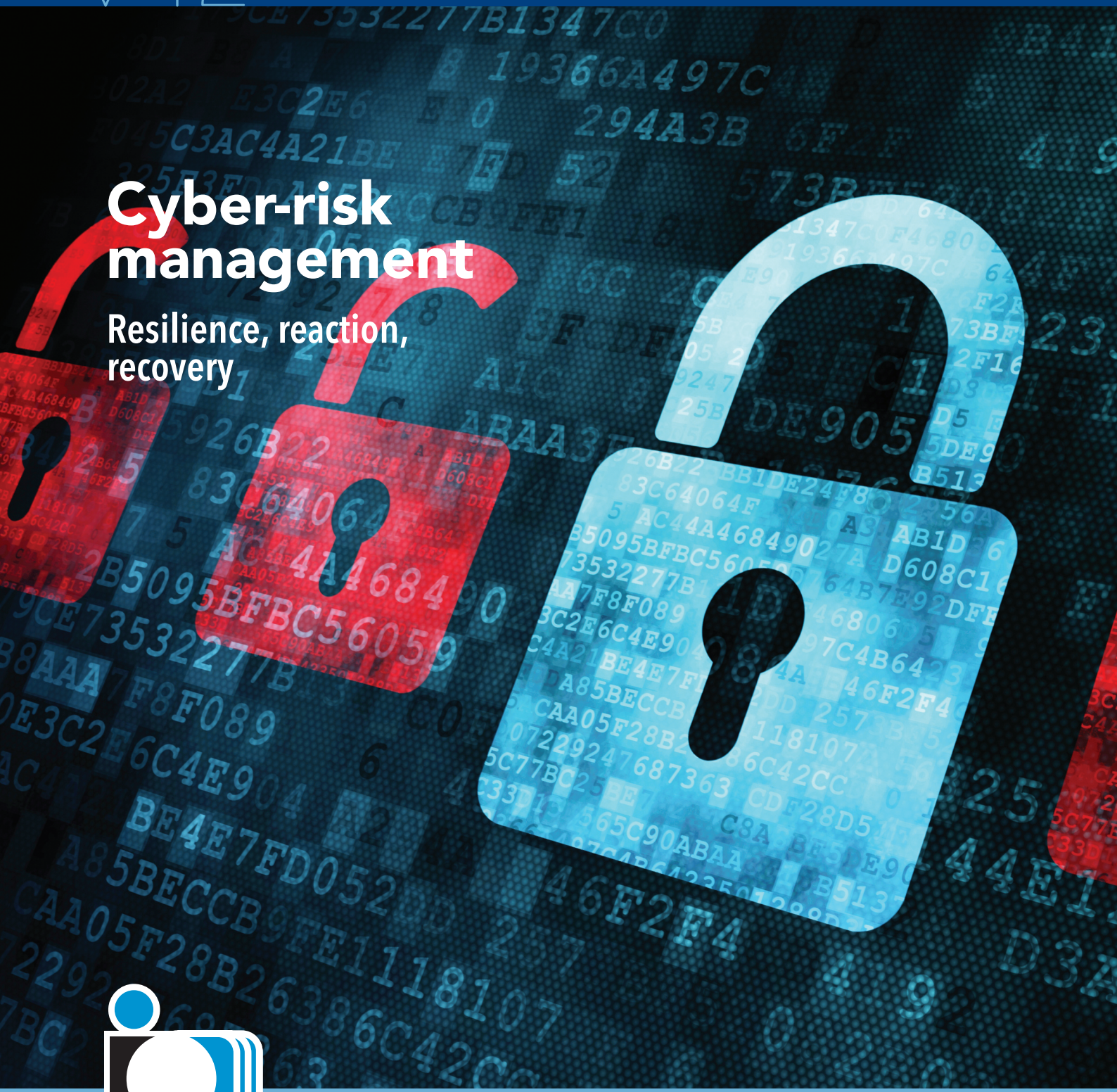
Published in:
Operations Management

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Operations Management

V42
www.iomnet.org.uk
Number 1 2016



Cyber-risk management

Resilience, reaction, recovery

THE INSTITUTE OF OPERATIONS MANAGEMENT

Getting the most out of your membership

Volunteering with IOM – see page 6

A systems approach to cyber-risk management

Companies do not have the resources to analyse every potential failure that faces the supply chain

A more comprehensive way of looking at cyber-risks in supply chains is required, particularly when considering the increasing complexity of logistics networks and their exposure to unexpected disruptions. This article explores why current risk assessment methods are insufficient, and provides an analogy for understanding the dynamic effects in a company.

Increased complexity in supply chains is exposing organisations to new risks. Many of these risks originate from the increasing dependence on information technology (IT) by competitive logistics networks. Organisations are being damaged by the resulting disruption of operations, as well as loss of company data, intellectual property and organisational value. Studies have shown costs at over $550 billion annually.[1] These disruptions are challenging the way we organise our operational activities, as well as the way we manage relationships with our partners. It also signifies that the transparent and rapid access to logistics resources enabled by IT is also a platform used by intruders for their own benefit.

The diversity of potential disruptions means that traditional risks assessment tools are impractical. Companies do not have the resources to analyse every potential failure, and to update the assessments as new risks appear, or existing risks change.

Our research at the Technical University of Denmark (DTU) is leading us to challenge the traditional risk analysis used in complex supply chains. Improvements can be achieved by moving from a static analysis, based on analysing reliability of components, to a dynamic analysis, based on control of vulnerabilities in the organisation – see Figure 1.

Although this novel approach requires a change in the way these risks are understood, it can create a comprehensive way of understanding the supply chain structure, and for improving supply chain reaction and recovery (resilience) when an unexpected cyberattack occurs.

Shortcomings in current approaches

The Federal Aviation Administration in the USA recently identified more than 100 methods for assessing risks[2], several of which are traditionally used in logistics networks. These methods are largely based on the premise that an undesirable event is caused by a chain of other preceding events. These methods are based on the assumption that these events can be decomposed, and that this decomposition allows for the independent analysis of each component, which does not influence the outcome. The process is known as analytic reduction. These analyses view this undesirable event and go backwards through the events that led to it, until the event that is considered the originator of the chain (the so-called root cause), is identified. This is the case of methods such as Failure Mode and Effect Analysis (FMEA) or Failure Mode and Criticality Analysis (FMECA), and are also known as backward-looking analyses. If instead an analysis is made to reveal all the possible chains of events in which something can go wrong, methods such as Failure Tree Analysis (FTA) are used. These are known as forward-looking analysis methods. Several other forward-looking methods are also widely used, such as Hazard and Operability Analysis (HAZOP) and Event Tree Analysis (ETA).

All of these methods follow the chain-of-failure-event causality model, which can be best represented through

The diversity of potential disruptions means that traditional risks assessment tools are impractical. Companies do not have the resources to analyse every potential failure, and to update the assessments as new risks appear, or existing risks change.

the analogy of a row of falling dominoes. There is an initial domino, labelled the root cause, that represents a single event. It could be a human error or a component failure. This error then propagates through the system, leading to other component failures and eventually making the last domino fall, where the problem is experienced – see Figure 2.

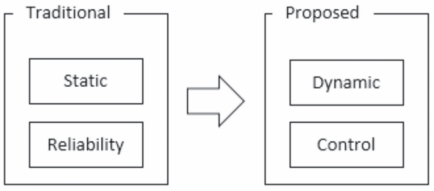
This family of methods have been widely used since their invention in the 1950s. They are popular due to their relative simplicity, and are effective in systems with technical components, as well as in simple systems involving both technical components and people, the so-called sociotechnical systems. A traditional way of quantifying cyber-risks would be to identify all the ways a logistics network could fail (reliability analysis) or be subject to cyberattack. This is best done in close interaction with an experienced team from different parts of the supply chain under analysis. The team will then agree on the likelihood of occurrence for each of these possible failures (probability), and an approximate amount of money lost if these failures were to occur (severity). Impact would then be *probability x severity* for each of these failures. By multiplying these two factors, a ranking of failures can be obtained, the events with highest impact can be identified and actions can be concentrated on elimination or mitigation of these risks.

Our research is leading us to question several assumptions about how new risks such as cyber-risks can be managed, due to the increased occurrence of different types of cyberattacks with potentially harmful effects on supply chain performance. We have thus searched for new ways of understanding these risks, and that has enabled us to develop practical proposals that could be useful to practitioners.

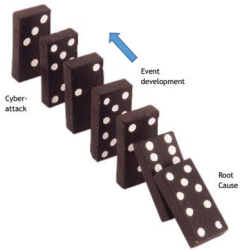
The traditional way of quantifying risks has several shortcomings. One of them has already been mentioned above. We will additionally analyse four other shortcomings[3]: reliability vs safety, subjective choice, systemic effects and dynamic behaviour.

Reliability vs safety

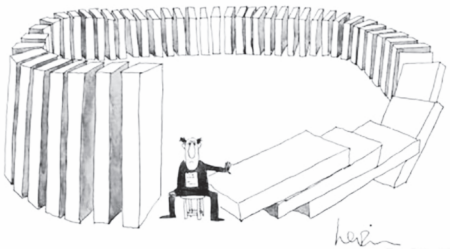
By focusing only on the performance of individual parts of the supply chain, there is the danger of confusing safety with reliability, meaning that it is generally assumed that if the components of the supply network function well, then the supply network is safe. This belief crumbles when errors occur in supply networks, where all components worked as expected, even sometimes because all components worked as expected. This can happen particularly where some type of redundancy has been built into the system, or where controllers (human or automatic) do not understand adequately what



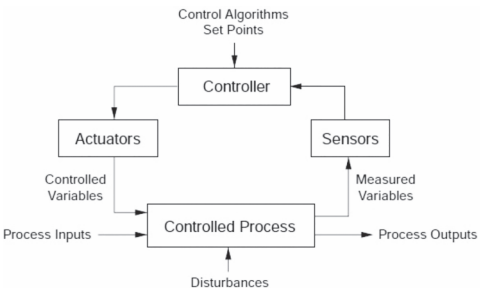
Proposed risk analysis change
Figure 1



Representation of the chain of failure as dominoes
Figure 2



Dangers when feedback loops are not considered
Figure 3



Control view of a process
Figure 4

actually happens in the process. Redundancy can work well in simple mechanical or electrical systems, but when it is applied to decision networks, it can lead, for example, to a double call, where two different people make contradicting decisions: a major problem in situations where urgent action is needed. Additionally, if the control actions in the procedures do not represent what should be done, a correctly functioning control procedure could lead to an unwanted disruption.

Subjective choice: who does the analysis?

In traditional risk assessment methods, there is a subjective choice of the chain of events. The list of potential failures – the chain of events leading to this failure, as well as the relationships between the events in the chain, right down to the root cause – is highly dependent on who is conducting the analysis. This can lead to several types of bias. If the participants are in management positions, without thorough knowledge of operations, then some relevant operational sources of accidents will be absent from the list. Root causes may be selected, just because they are politically acceptable, and other potential explanations may not be explored, because they could be an embarrassment for the organisation. Many times this search also ends with some type of operator error or lack of training. Jens Rasmussen, researcher, Risø (present DTU), mentioned in the 1980s that it is indeed very difficult to analyse through a perceived human error, and therefore the analysis stops there.

Systemic effects: look at the wider picture

Only a very limited chain of events is taken into account in these traditional methods, and factors not directly included in a chain of events are excluded. The explanation usually considers the events that immediately led to the loss and systemic factors are not considered. Systemic factors can be the consequences the decision has in other parts of the organisation, affecting and counteracting the original decision through feedback loops. This normally does not happen immediately – see Figure 3. The systemic effects can also include policy decisions in the company, leading to the unwanted disruptions.

A proper understanding of the required behaviour and the ability to withstand disruptions from cyberattacks and regain normal operating conditions (cyber-resilience) is hidden in the traditional methods. The reaction by the company, when having to cope with a cyberattack, will normally be a series of actions, using resources present in the company. These actions will develop over time, and the stability of the operation will eventually be restored. This will not happen immediately and it will take some time. This means that cyber-resilience is, in fact, a dynamic behaviour of the supply chain, and as such it requires a way to deal with these dynamics. Let us look at this more closely.

Dynamics can be better understood by comparing a manufacturing company subject to cyberattacks with a car on the road

Dynamics: businesses vs cars

Dynamics can be better understood by comparing a manufacturing company subject to cyberattacks with a car on the road. A company manager would be equivalent to the car's driver. Cyber-risks coming towards this company can be represented as obstacles on the road coming towards the car. The car has several controls that can be used by the driver to avoid these obstacles, such as the steering wheel, the accelerator and the brakes. In the same way, the company has also some controls that can be used by the manager to direct the company development, such as setting strategic objectives, investment in training or incentive structures towards collaboration with suppliers. The car has a mass that results in inertial effects. Due to the risk of a crash, it is not possible or convenient for the driver to change the car's direction suddenly, or accelerate, or stop the car suddenly. These inertial effects are also one of the characteristics for real systems, known as dynamic effects. The company has also inertial effects such as the number of employees, the total accounts payable or the number of electronic orders for products. This means that a manager cannot make sudden changes in the controls, in the case of risk of a cyberattack, without other consequences.

A driver avoids an obstacle in the road by using the controls – for example, activating the brakes at a forthcoming stop sign. A novice driver might attempt to break too late, thrusting him forward with a jolt: a not always gentle reminder of the inertial effect of our own mass in movement. In the case of the company, a manager, attempting to avoid the effects of a cyberattack will use the controls at his or her disposal. A novice manager may attempt to change strategic objectives too quickly or change the incentive structures radically, thereby creating an organisational jolt.

Unknown inertial effects

Some important differences come to light in this analogy, which we have defined as differences of management and differences of design. Drivers normally start driving (managing) the car from a resting position, and with training the driver will gradually explore increasing levels of driving difficulty. In the case of the company, the manager will usually be appointed to the role, with the company already 'in movement' at an undetermined speed. He will have a series of controls. Some of them will be familiar from previous experience, and some might be new controls, implemented by a predecessor.

There are different organisational masses, which the manager will not necessarily know about and will have to

discover by trial and error. Moreover, the manager will not have experience with the inertial effects that these available controls will have on the company. Finally, in the same way drivers are taught in the driving school about existing cars and driving conditions, managers are trained in business schools about existing companies and business conditions.

Another important and very relevant difference is one of design. The car has a structure, developed and improved over time by a team of specialists. They understand the effects this car structure has on the car's behaviour, with special attention to dynamic effects. The structure of a company will usually not have been designed, but rather replicated initially from other working models, maybe grown through acquisition of other companies (inorganic growth) or through its own expansion (organic growth). Company structures are therefore very likely to develop without any design considerations to its dynamics.

Control view of risks

Taking the car analogy further, resilience, or the ability to return to normal operations after disruptions, can be then understood as the ability of the company to adjust it course (its processes) by using its control structures – see Figure 4. Resilience would then be reflected in how well this control structure works by:

- How well and timely sensors measure the current process
- How well and timely we act on the process with our actuators when there is something to be done
- How well and timely our supply chain can translate what it is sensing into what it has to do about it, through its controller

This is an ongoing activity, since the supply process is constantly encountering different working conditions that have to be detected and be adapted to

Steps to implement the control view

Supply chain cyber-resilience through the control view of cyber-risks can be achieved by the following general steps:

- Identify what the company will consider as undesirable disruptions to the supply chain – identify potential accidents
- Identify the mix of conditions in the current supply network that would lead to the undesirable disruptions specified in the previous step – identify hazards
- Define the boundaries of what is in control and out of the control of the company – identify supply system boundaries, controls and masses present in the system
- Brainstorm about how each potential disruption identified in the first step could occur; this will lead to the identification of potential improved controls, which should be in place – for example, how the process is measured (sensors), organisational structures (actuators), or action plans for crisis management teams (controllers)

About the authors

Daniel Sepulveda, MSc. PhD Researcher at Management Engineering at the Technical University Denmark. (DTU). His current topic of research is cyber-risk and security in the global supply chain, under the guidance of Professor Omera Khan. He has worked in supply chain management for over 12 years in operational and strategic positions and has experience with multinational companies in five continents.

Email: dasep@dtu.dk

Omera Khan FCILT is Professor of Operations Management, Technical University of Denmark (DTU) and is also Visiting Professor and Programme Director of the MSc in International Supply Chain Management at Royal Holloway University of London. In addition to leading a number of ongoing research projects, she works with organisations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chain and operations management.

Email: okhan@dtu.dk

References

1. 'Netlosses: Estimating the global cost of cybercrime', www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf
2. Federal Aviation Administration (2008), 'System safety handbook', retrieved 24th September 2015, www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/
3. Other shortcomings of the use of traditional risk assessment methods in supply networks, which are not analysed in detail in this article, include aspects such as: their excessive search for guilt and operator error, instead of understanding the structure of the system that led to the disruption; assuming that two different events leading to a disruption will happen independently of each other, when analysing how likely they are to happen, merely for mathematical simplicity; or the risk of hindsight bias – that is, the perception of the disruption as foreseeable when looked after the fact, changing the discussion to what was done wrong instead of the more fruitful one of why it made sense for the operators to make that decision at that time.